Reliable and Secure Group Communication

PI: Deb Agarwal

Karlo Berket, Olivier Chevassut, and Quang Dinh

Distributed Systems Department
Lawrence Berkeley National Laboratory

11/28/2001

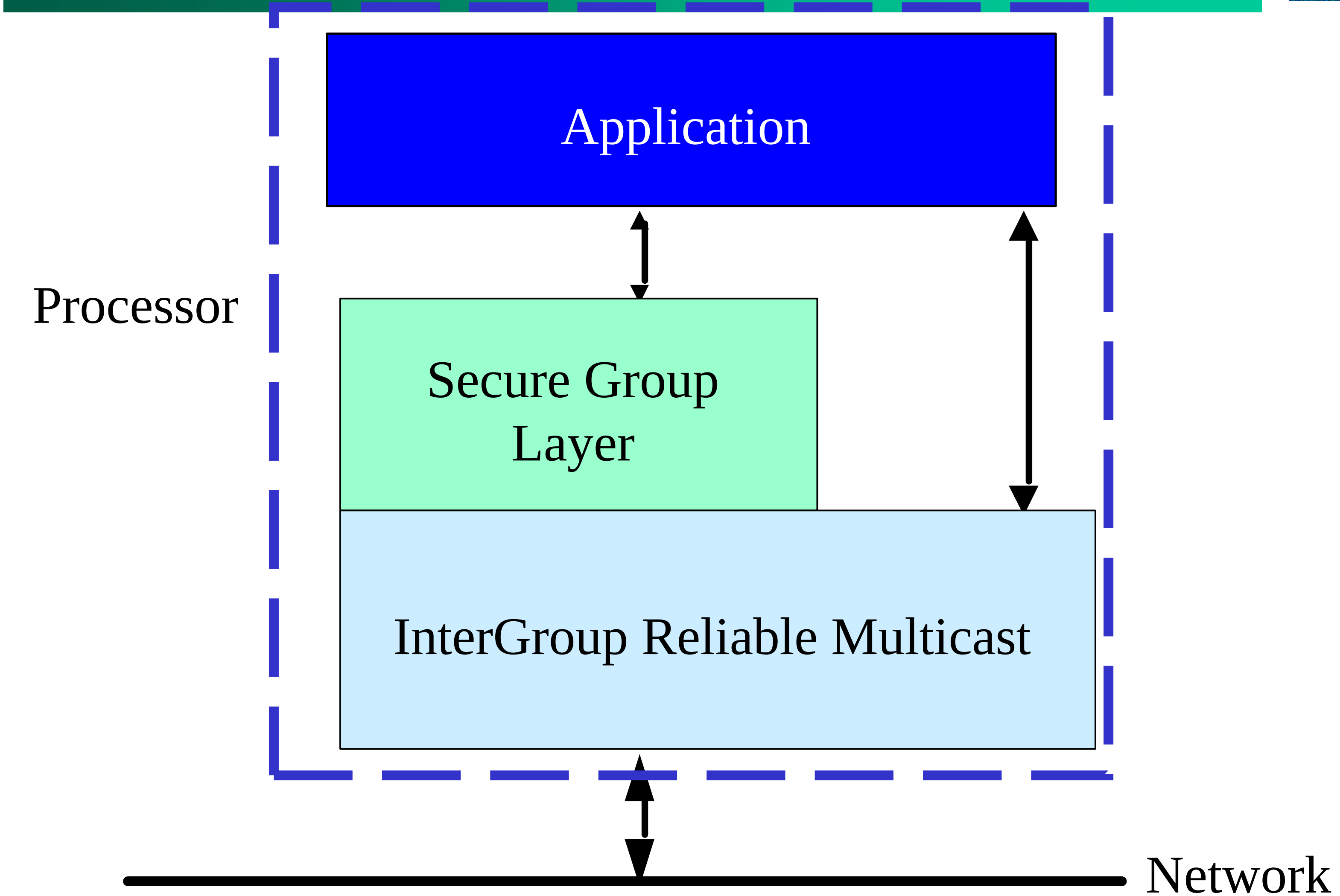
Peer-to-Peer Model

- Allow ad-hoc collaboration
- Remove centralized servers
  - scalable to large collaborations
  - remove bottleneck
- Better model for many collaborations – no natural central authority
- Easy to add new resources to the collaboration
  - minimize setup required
  - allows local control over resource authorization

Group Communication Goals

- Provide reliable communication for collaborating groups spread across the Internet
  - simplify distributed application development
  - simplify communication between components in distributed applications
  - support flexible delivery capabilities to support a broad range of application needs (e.g., ordering)
- Provide a secure channel among the group members with security services similar to SSL
  - support confidentiality, authenticity, integrity
  - support access control based on membership authorization (individually enforced)
  - security services optional

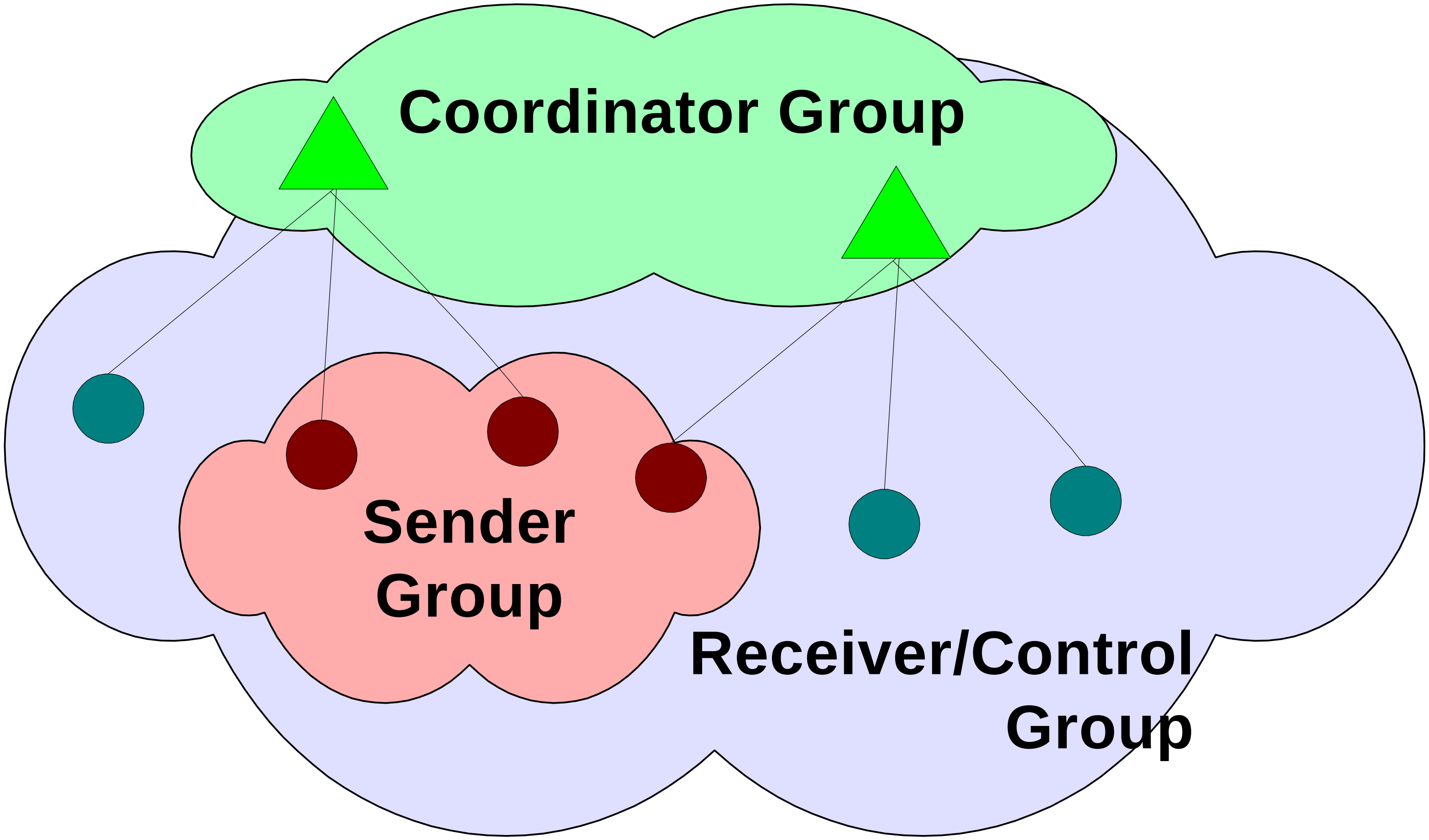
System Design



InterGroup Reliable Multicast

- Membership divided into senders and receivers
- Receiver oriented selection of delivery service
  - FIFO order, causal order, or timestamp order
  - Membership changes delivered in order
- Control hierarchy
  - Scalable collection of status information
  - Maintain coordination with receivers

InterGroup Schematic



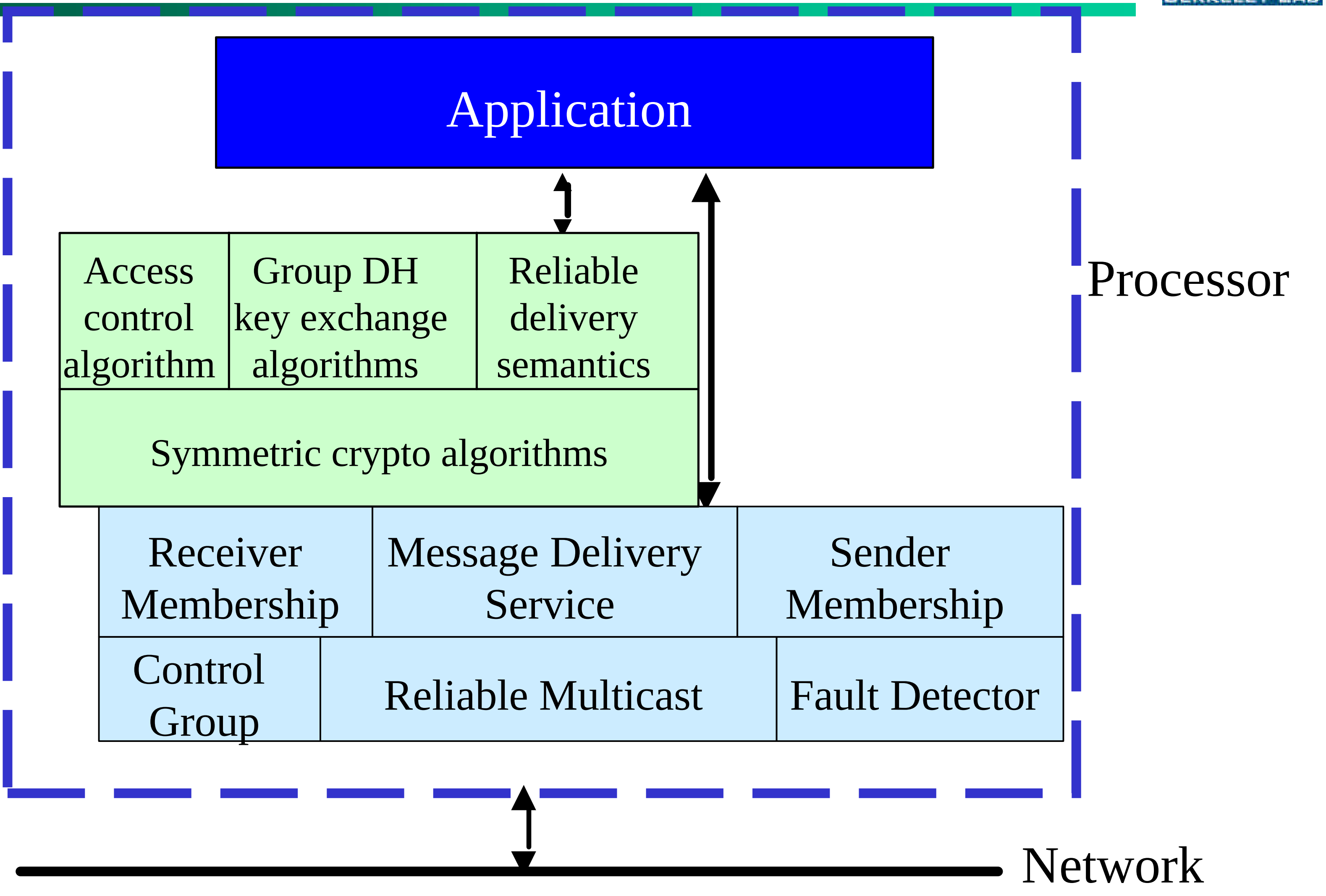
Secure Group Layer (SGL)

- Support dynamic membership
  - members join and leave the group at any time (e.g., network partitions and merges)
  - membership is not known in advance
- Achieve strong security goals
  - authenticated key exchange (AKE)
  - mutual authentication (MA)
  - forward secrecy (FS)
- Provide an SSL-like secure channel

Project Milestones

- Year 1
  - InterGroup testing and improvements
  - Begin development of example applications
  - Publish proof of security for SGL key exchange algorithms
  - Limited prototype implementation of SGL using the InterGroup protocols
- Year 2
  - Beta release of InterGroup implementation
  - Improvements to membership and message delivery
  - Publish a security analysis of SGL
  - Release SGL using InterGroup protocols (sender group mode)

System Design



Application

Access control algorithm

Group DH key exchange algorithms

Reliable delivery semantics

Symmetric crypto algorithms

Receiver Membership

Message Delivery Service

Sender Membership

Control Group

Reliable Multicast

Fault Detector

Processor

Network